**7.1.4.2.1. Subject Alternative Name Extension**

Certificate Field: extensions:subjectAltName

Required/Optional: Required

Contents: This extension MUST contain at least one entry where each included entry is one of the following:

**7.1.4.2.1.1. dNSName**

The subjectAltName extension MAY include one or more dNSName entries provided each entry is either a Fully‐Qualified Domain Name or a Wildcard Domain Name. The CA MUST verify each Fully-Qualified Domain Name and Wildcard Domain Name entry in accordance with Section 3.2.2.4.

Except where the entry is an Internal Name using onion as the right‐most label in an entry in the subjectAltName Extension or commonName field in accordance with Appendix F of the EV Guidelines, a dNSName entry MUST NOT contain an Internal Name.

**7.1.4.2.1.2. iPAddress**

The subjectAltName MAY include one or more iPAddress entries provided each entry is an IP address verified in accordance with Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.

**7.1.4.2.1.3. rfc822Name**

The subjectAltName MAY include one or more rfc822Name entries provided each entry is an email address compliant with RFC5280. Prior to including an email address, the CA MUST take reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate orhas been authorized by the email account holder to act on the account holder’s behalf.

**7.1.4.2.1.4. otherName with SRVName { 1.3.6.1.5.5.7.0.18.8.7 } type-id**

The subjectAltName MAY include one or more SRVNames (as defined in RFC4986) as an otherName entry with the SRVName type-id. The CA MUST verify the name portion of the entry in accordance with Section 3.2.2.4. SRVName entries MUST NOT contain Wildcard Domain Names. If a Technically Constrained Subordinate CA Certificate includes a dNSName constraint but does not have a technical constraint for SRVNames, the CA MUST NOT issue certificates containing SRVNames from the Technically Constrained Subordinate CA Certificate. A Technically Constrained Subordinate CA Certificate that includes a technical constraint for SRVNames MUST include permitted name subtrees and MAY include excluded name subtrees.

**7.1.4.2.1.5. otherName with id-wfa-hotspot-friendlyName { 1.3.6.1.4.1.40808.1.1.1 } type-id**

The subjectAltName MAY include one or more entries of the id-wfa-hotspot-friendlyName type-id. The CA MAY only include id-wfa-hotpost-friendlyName entries compliant with the Hotspot OSU Certificate Policy as officially published by the Wi-Fi Alliance at [https://www.wi-fi.org](https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint). Prior to including a id-wfa-hotpost-friendlyName entry, the CA MUST:

1. Authenticate the authority of the certificate requester in accordance with Section 3.2.5;
2. Authenticate the Subject Identity information in accordance with Section 3.2.2.1; and
3. Conduct a trademark search for the entry with the U.S. Patent and Trademark Office and equivalent international trademark office such as the WIPO ROMARIN.